CS/ECE/MATH 435 FINAL, SPRING 2012

Nigel Boston

For full credit you must explain your reasoning (except in question 1). Clearly written partial answers will also receive partial credit. Answer the questions in any order.

1. Are the following statements true or false? No justification is needed for your answers to this question.

(a) If the index of coincidence of an encrypted text is 0.04116, then it was probably encrypted by a monoalphabetic cipher.

(b) The person receiving an RSA digital signature sets up the instance of RSA used.

(c) The entropy of the English language constrains the factor by which a cryptographic hash function can compress English text.

(d) AES does not use Feistel ciphers.

2. (a) Carefully define the three main attacks on general cryptosystems (depending on how much we know about the plaintext etc.). Explain how we might cryptanalyze a substitution cipher in each of those three cases.

(b) How many keys are there for the following cryptosystems, acting on the English alphabet? (i) Shift ciphers. (ii) Affine ciphers. (iii) Substitutiion ciphers. How many keys does DES have?

(c) If we do double encryption, so that $y = e_{k_2}(e_{k_1}(x))$ gives the ciphertext y in terms of the plaintext x, how many keys are there in the case of affine ciphers? In the case of DES, why does double encryption also not greatly increase the security?

3. (a) In preparation for encryption, an English text containing 1000 letters is converted to blocks containing 5 bits each by $A \to 00000, B \to 00001, C \to 00010, ..., Z \to 11001$, space $\to 11010$. Explain how, with a little more cleverness, it can be converted into a lot fewer than 5000 bits. What is the approximate minimum number of bits into which it is possible to compress the text reversibly?

(b) A 7-letter text is then encrypted using the key stream from a 4-cell Linear Feedback Shift Register, yielding output 10000101000111000101011000101110100. If we happen to know that the input bits start 00001000, then find the start of the key stream, the LFSR, its period, and what the original message was (in letters).

(c) Explain Kasiski's method. The output of a Vigenere encryption is KZEJAXKZSZUKJZEZCSJAXKZSYWEGKSZUK. What is the likely keyword length?

4. (a) Suppose that a and b are relatively prime positive integers. Explain how the extended Euclidean algorithm produces integers u, v such that $ua+vb = 1$. Use this to compute the multiplicative inverse of 19 (mod 26).

(b) Alice and Bob set up RSA systems with the same modulus N, but different encryption exponents a, b respectively. Suppose that a and b are relatively prime. Charles sends them each the same message m $(1 < m < N)$. Show that if Eve intercepts both of Charles' transmissions, then she can compute m. [Hint: use part (a).]

(c) A Hill cipher encrypts blocks of letters of length 2 by multiplying them by the matrix $\begin{pmatrix} 5 & 1 \\ 1 & 4 \end{pmatrix}$ (mod 26). Find the decryption map.

5. (a) Describe in detail how Alice and Bob set up an elliptic curve Diffie-Hellman key exchange. Be careful to specify what is public and what private.

(b) Suppose Eve cannot only observe messages between Alice and Bob, but can also intercept them and replace them with messages of her own. Say Alice and Bob are setting up a Diffie-Hellman key exchange. Show that Eve can impersonate Alice to Bob and impersonate Bob to Alice, with neither of them suspecting. [This is not a hard question, but give details.]

(c) Alice and Bob wish to use the elliptic curve $y^2 = x^3 + x + k$ over $\mathbf{F}_{65537}$ for some choice of k. For simplicity, they decide to use $P = (0, 0)$ to set up the key exchange. What must k be? Why is this choice of P a bad one? What is $2P$?